Phishing Guard and Antivirus: A New Approach

B. Sadeghi Bigham¹, S. Chernin¹, A. Madadi², N. Madadi³, P. Tavajoh¹

¹ Faculty of Information Technology, Institute for Advanced Students in Basic Sciences (IASBS)
Zanjan Iran.

² Mathematics and Computer Group, Educational organization, Tehran, Iran.

³ Mathematics department, Semnan university, Semnan, Iran.

Abstract - *One of the simplest ways to violate private bounds of individuals in digital world is "Phishing". Several methods have been introduced in order to confront with these abstruse phenomena, which we can say that none of them has been truly successful. In this essay we shall proceed with a new method, in which with the help of an Anti-virus, defeating "Phishing" would be possible. In the presented method introduced by us the subject of Users trust and reliance by using anti-virus is high lighted. In the past, using anti-virus was one of the ways to confront with "Phishing", but our procedure can improve previous methods, and can reduce the possibility of Users being trapped.*

Keywords: Hack, Security, Antivirus, Phishing, Guard.

SAM'08: The 2008 International Conference on Security and Management

1 Introduction

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait.

Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims. In one fairly typical case before the Federal Trade Commission (FTC), a 17-year-old male sent out messages purporting to be from America Online that said there had been a billing problem with recipients' AOL accounts. The perpetrator's e-mail used AOL logos and contained legitimate links. If recipients clicked on the "AOL Billing Center" link, however, they were taken to a spoofed AOL Web page that asked for personal information, including credit card numbers, personal identification numbers (PINs), social security numbers, banking numbers, and passwords. This information was used for identity theft. In this paper we are going to suggest a new

way to improve the antivirus systems in order to identify the phishing traps. By using such a method users can safely surf the internet.

2 A brief history of Phishing

Before mid-2003, most phishing scams arrived in text-heavy e-mails. They were rife with spelling errors and poor grammar that tipped recipients off. But phishers are honing their writing and design skills, creating messages that are more difficult to discern as forgeries. Here is a brief timeline of the development of phishing. E-mail fraudsters register dozens of look-alike domain names, such as yahoo-billing.com and ebay-fulfillment.com. They also create Web sites that contain the names of well-known companies and brands like microsoft.checkinfo.com. Researchers have developed models and guidelines on fostering online consumer trust [1, 3, and 4]. Existing literature deals with trustworthiness of website content, website interface design and policies, and mechanisms to support customer relations. None of these papers consider that these indicators of trust may be spoofed and that the very same guidelines that are developed for legitimate organizations can also be adopted by phishers.

Empirical research in online trust includes a study of how manipulating seller feedback ratings can influence consumer trust in eBay merchants [2]. Fogg et al. conducted a number of large empirical studies on how users evaluate websites [6, 7] and developed guidelines for fostering credibility on websites, e.g., "Make it easy to verify the accuracy of the information on your site" [5]. After giving up personal and financial information on a phishing site, the victim is redirected to the real homepage of the company being targeted. Experts say this psychological trick helps erase doubts that victims may harbor about the veracity of the experience and allows more people to be swindled. This tactic is a standard feature of scams today. New scams impersonate the Department of Homeland Security, the Internal Revenue Service and the Federal Deposit Insurance Corporation. Phishers devise a new way to dress up what is typically the weakest part of their scams: the dubious Internet addresses that appear in the victim's Web browser when he or she clicks on the link in a phishing e-mail. Novel programming tricks alter the appearance of the victim's

address bar by replacing the URL of the phishing site with that of the company being impersonated.

Figure 1 shows the number of phishing attacks in different hosts around the internet, which are at the high rank of visiting sites around the internet.

Figure 1: The number of phishing attacks in different hosts around the internet, which are at the high rank of visiting sites around the internet.

3 Phishing guard

In this part we shall proceed on a new method, which will not under estimate any previously done actions and works by any means, but can be considered as a complementary in this subject. This method can specifically be used with previously presented Anti-viruses. In this method we will consider the Users reliance to Anti-Virus packages, organize an Informational Bank, which will be up dated and has the ability to Login, up dated caution signs. There are some methods in order to confront with "Phishing" phenomena, which seem to be practicable, but unfortunately because of the repetitious aspects and unsuitable specifications of messages, they do not leave any impression on the Users, and will be disregarded easily by them. For example in the Iranian Site (Persian Language) "Cloob.com", after indicating the "User name" and "Password" and clicking, a new page will be opened in the place of the "User name" and "Password" which has the following message "Please take note that the website of Cloob is www.cloob.com", afterwards the place for indicating "User name" and "Password" will move to another side of this webpage and by indicating the required datum you can login. This method has two big disadvantages, which will subtract the efficiency of this method.

3.1 The First Disadvantage

This message will become repetitive for the User and normally and habitually they will double click : Once in the first place of "User name" and immediately for the second

time in the second and main place of the "User name" and will not read the message at all.

3.2 The Second Disadvantage

The sketcher of "Phishing" has designed the same plan, therefore you can not recognize any differences between this design with the original main page, and this could be the second aforesaid disadvantage.

Due to separated researches in the mentioned site we have realized that approx. 90% of the Users have never read or paid any attention to this message (In fact they have considered this message as a failure of the website design and have rapidly double clicked in this page) and approx. 9.6% have only read this message a number of times and have paid attention to the mentioned site address indicated in this message. This is while experimentations have shown that applying an Anti-virus with circumstantial cautions, will increase the sensitivity of the Users and will stimulate them to read the message, partly with a sense of anxiety and dread. The above mentioned subject needs no substantiation and can easily be accepted without representing any statistics. Concerning the capability of Anti-viruses in confronting "Phishing" phenomena there is a major disadvantage which will be discussed in the below.

As noted before the caution signs applied by anti-viruses in confronting "Phishing" will be taken really seriously by the Users. The only point that causes apprehension is that the sites which apply "Phishing" will be defined as an offender by Organizations and Companies and their Web addresses will be added to the banded Website addresses located in the anti-virus informational bank. The user will regularly update his anti-virus in his computer, and this procedure will become time consuming, which can be considered as the major disadvantage of this method. In our new demonstrating method as we will use the reliability of the User (As a point of authority) we will try to re-solve the above mentioned disadvantage.

3.3 The new solution

In our method we will assume a new capability, added to an anti-virus, in which alters the anti-virus as a safe guard against "Phishing" attacks. This anti-virus will have an informational bank, consisting of relevant "Phishing" addresses. At the meantime, such Anti-viruses, with the above mentioned capability do exist. The novel section, is that when ever the User logs in a new page, the anti-virus will define this login and will send a message as follow:

("[This is the first time you have entered in to this web page. Does the site address accord, with your favored address?]")

Also in order to increase the percentage of safety, and considering the possibility of the caution not being read by

the impatient User, we can define for the "Enter button" the answer "NO", and consequently, avoid login. In case the answer of the User to the above question is positive, the Anti-virus will set the website address in to its informational bank, and shall not repeat the question in the next visits of the User to this site. The accumulation of the datum in informational bank will greatly decrease the number of this question being asked, and as a result the reliability of the User will not be underestimated and ruined. (This question will be asked for each website only one time). On the other hand in order to diminish the number of repetition of this question, we can stipulate a number of popular login addresses, simultaneously, while producing the anti-virus. Here below you can find a general sketch of this method:

A general sketch concerning up dating, an anti-virus informational bank

Step 1: Distinguishing, login of the User.

Step 2: Picking up the site address by anti-virus.

Step 3: If the site address is already indicated in the informational bank of anti-virus, the algorithm will be finalized.

Step 4: Anti-virus will present the following message to the User, and will wait for his response. ("[This is the first time you have login, in to this web page. You might be at the risk of "Phishing", please re-control your required website address. Are you sure you want to login?]")

Step 5: If the answer to this question is positive ("[YES]"), add the website address to the anti-virus informational bank, and set the User to freely enter the website. Otherwise, do not add the address to the anti-virus informational bank, exit and avoid entrance.

Two major problems will remain, which should be regarded in anti-virus program writing.

1-How can an anti-virus distinguish that the User is logging in.

2-When should the anti-virus, restrict the User from further activity, and take away the Users permission for entering, or clicking.

To solve the first mentioned problem, the programmer should write his program in a manner that when ever the typed characters by the User is not coordinated to the represented characters in the webpage, login is authorized and the process starts. There are several solutions for solving the second problem. One of the proven method's is, that in the first time of entering in to the website, the password process is activated and will remain activated until the password is given by the User, and the message can also be displayed.

During this process, the User should not face with any interruption while typing his password, and the duration for typing the password should be to the extent of completion of the Anti-virus process. For example if the password only consists of one character, and the enter button is clicked immediately by the user, there would be no chance for the anti-virus to process and the user will be trapped. Although, with consideration of the high speed of Anti-virus being process, while limiting the User's utilization of "minimum" character for password, the above mentioned condition will not be an abstruse problem and the suggested method seems effectual.

4 Conclusion

In this paper, after contemplating "Phishing" abstruse phenomena we have represented methods to confront with this problem, we have up to now, pointed out the advantages of using Anti-viruses. We presented a new method, based on Anti-viruses, in which the User would up date the anti-virus in his personal computer and the caution message will alert him in moments of eventual danger. Thus the number of these warnings would be very limited, and they would become so factual, that the warning messages will not put the credibility of anti-viruses underestimation. The anti-virus, will distinguish the time of login and will compare the address of the website with previously web pages, defined as licensed. In case the webpage has been visited for the first time by the user, the anti-virus will give a caution message, and shall simultaneously up date its informational bank. This method could be applied in the design of future coming anti-viruses.

5 References

- [1] 1. Ang, L., C. Dubelaar, & B. Lee. To Trust or Not to Trust? A Model of Internet Trust from the Customer's Point of View. *Proc. 14th Bled E-Commerce Conf.* (2001), 25-26.
- [2] 2. Ba, S. & P. Pavlov. Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. *MIS Quarterly*, 26, 3 (2002), 243-268.
- [3] 3. Cheskin Research. *E-commerce Trust Study* (1999).
- [4] 4. Egger, F.N. Affective Design of E-commerce User Interfaces: How to Maximize Perceived Trustworthiness. *Proc. Intl. Conf. Affective Human Factors Design* (2001), 317-324.
- [5] 5. Fogg, B. J. Stanford Guidelines for Web Credibility. *Res. Sum. Stanford Persuasive Tech. Lab.* (2002).
- [6] 6. Fogg, B. J. et al. How Do Users Evaluate the Credibility of Web Sites: A Study with Over 2,500 Participants. *Proc. DUX* (2003).

[7] 7. Fogg, B. J. et al. What Makes Web Sites Credible: A Report on a Large Quantitative Study. *Proc. CHI* (2001), 61-68.